Amendments to the Claims:

This listing of claims replaces all prior versions, and listings, of claims in this application.

Listing of Claims:

1. (Currently amended) A method for performing an electronic transaction between a first transaction party and a second transaction party using an electronic device operated by the first transaction party, the method comprising:

providing authentication data in a memory of said electronic device which authentication data are inaccessible to a user of said electronic device;

providing authentication software in said electronic device, the authentication data being accessible to said authentication software;

activating the authentication software to generate a digital signature from the authentication data;

providing the digital signature to the second transaction party,

wherein the digital signature is generated by:

gathering session-specific data;

hashing said session-specific data to obtain reference numbers referring to positions in the authentication data stored in said electronic device; and

generating the digital signature from the characters stored in the authentication data at said positions.

2. (Previously presented) The method according to claim 1, wherein the second transaction party provides digital data to the first transaction party.

3. (Previously presented) The method according to claim 2, wherein the second transaction party embeds the digital signature in the digital data provided to the first transaction party.

4. (Previously presented) The method according to claim 1, wherein the second transaction party stores the digital signature together with data identifying the first transaction party.

5. (Previously presented) The method according to claim 1, wherein the authentication data are provided by the second transaction party, which stores the authentication data together with data identifying the first transaction party.

6. (Cancelled)

7. (Currently amended) The method according to claim 5 ~~6~~, wherein the second transaction party verifies the digital signature provided by the first transaction party using the authentication data stored at the second transaction party.

8. (Currently amended) The method according to claim 1, wherein the first transaction party further provides a signed digital signature to the second transaction party, the signed digital signature being generated by the authentication software by signing the digital signature using a private key, which private key is unique for said authentication software and is provided by ~~known to~~ a trusted third party, and is not known to the second transaction party.

9. (Cancelled)

10. (Currently amended) The method according to claim ~~1~~ 5, wherein the authentication data are encrypted by the second transaction party using an encryption key before the authentication data are provided to the first transaction party.

11. (Previously presented) The method according to claim 10, wherein the authentication software retrieves a decryption key associated with the encryption key and decrypts the authentication data at a first use of the authentication data.

12. (Previously presented) The method according to claim 1, wherein said memory is inaccessible to an operating system of said electronic device, thereby rendering the authentication data inaccessible to said user.

13. (Previously presented) The method according to claim 12, wherein the authentication data are provided in a Basic Input-Output System (BIOS) of the electronic device.

14. (Previously presented) The method according to claim 1, wherein the authentication data are encrypted when the authentication data are stored in said memory, and wherein a decryption key for decrypting the authentication data is inaccessible to said user and to any user-operated software, thereby rendering the authentication data inaccessible to said user.

15. (Previously presented) The method according to claim 14, wherein the authentication data are encrypted using at least two encryption layers.

16. (Previously presented) The method according to claim 15, wherein at least one encryption layer may be decrypted using a decryption key associated with at least one serial number of a hardware components of said electronic device.

17. (Previously presented) The method according to claim 15, wherein at least one encryption layer may be decrypted by the authentication software.

18. (Previously presented) The method according to claim 14, wherein the authentication data are decrypted in a secure processing environment inaccessible to said user and to any user-operated software.

19. (Previously presented) The method according to claim 1, wherein the authentication data comprise an authentication table.

20. (Previously presented) The method according to claim 19, wherein the authentication table is generated from a bit string which is generated from fixed data and variable data.

21. (Previously presented) The method according to claim 20, wherein the fixed data are at least part of a serial number of a hardware device.

22. (Previously presented) The method according to claim 20, wherein the fixed data are at least part of a device specific software identification code of the authentication software.

23. (Previously presented) The method according to claim 20, wherein the variable data comprise a random table.

24. (Previously presented) The method according to claim 23, wherein the random table is calculated from a random two-dimensional or three-dimensional pattern.

25. (Previously presented) The method according to claim 19, wherein the authentication table is generated from fixed data, variable data and a bit string, which bit string is specific to a trusted third party that provides the authentication data.

26. (Previously presented) The method according to claim 1, wherein the authentication software is stored in a secure memory location inaccessible to an operating system.

27. (Previously presented) The method according to claim 1, wherein the authentication software is run in a secure processing environment inaccessible to an operating system.

28. (Currently amended) A method for encrypting digital data on an electronic device using an encryption key, the method comprising:

gathering session specific data;

hashing said session specific data to obtain reference numbers referring to positions in ~~an~~ authentication data ~~table~~ stored in said electronic device;

generating said encryption key from the characters stored in the authentication data ~~table~~ at said positions; and

encrypting said digital data using said encryption key.

29. (Currently amended) A system for performing an electronic transaction between a first transaction party and a second transaction party using an electronic device operated by the first transaction party, the system comprising:

means for providing authentication data in a memory of said electronic device which authentication data are inaccessible to a user of the electronic device;

means for providing authentication software in said electronic device, the authentication data being accessible to said authentication software;

means for activating the authentication software to generate a digital signature from the authentication data;

means for providing the digital signature to the second transaction party; and

means for providing digital data from the second transaction party to the first transaction party,

wherein the means for activating the authentication software to generate a digital signature from the authentication data comprise:

means for gathering-session specific data;

means for hashing said session-specific data to obtain reference numbers referring to positions in the authentication data stored in said electronic device; and

means for generating the digital signature from the characters stored in the authentication data at said positions.

30. (Cancelled)

31. (Currently amended) A system for encrypting digital data using an encryption key, the system comprising:

means for providing authentication data in a memory of said electronic device which authentication data are inaccessible to a user of the electronic device;

means for providing authentication software in said electronic device, the authentication data being accessible to said authentication software;

means for activating the authentication software to generate a digital signature from the authentication data;

means for gathering session specific data;

means for hashing said session specific data to obtain reference numbers referring to positions in ~~an~~ the authentication data ~~table~~ stored in said electronic device;

means for generating said encryption key from the characters stored in the authorization ~~table~~ data at said positions; and

means for encrypting said digital data using said encryption key.

32. (New) A system for performing an electronic transaction between a first transaction party and a second transaction party using an electronic device operated by the first transaction party, the system comprising:

means for providing authentication data in a memory of said electronic device which authentication data are inaccessible to a user of the electronic device;

means for providing authentication software in said electronic device, the authentication data being accessible to said authentication software;

means for activating the authentication software to generate an encryption key from the authentication data;

means for encrypting digital data using the encryption key to provide encrypted digital data; and

means to provide the second transaction party with said encrypted digital data,

wherein the means for activating the authentication software to generate an encryption key from the authentication data comprise

means for gathering session specific data;

means for hashing said session specific data to obtain reference numbers referring to positions in the authentication data stored in said electronic device; and

means for generating the encryption key from the characters stored in the authentication data at said positions.